

21 JUL 2005

PCT/GB 2003 / 0 0 4 3 7 7



10/1431



INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

REC'D 15 DEC 2003

WIPO

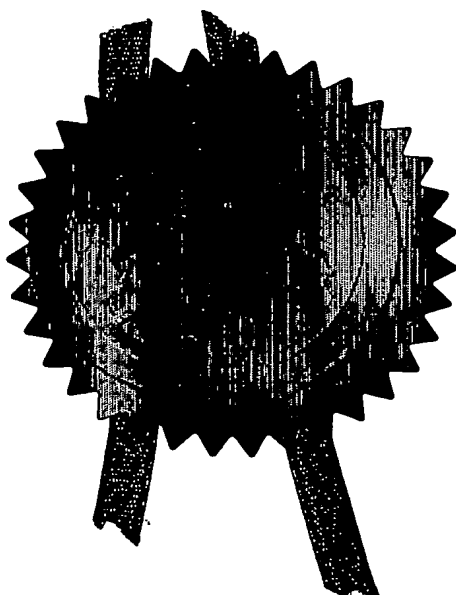
POT

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.



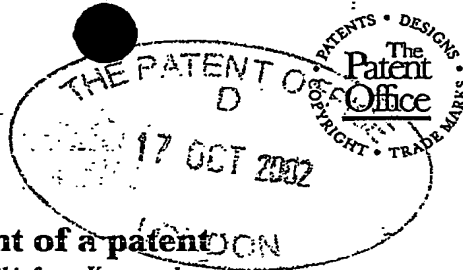
Signed

Dated

25 November 2003

**PRIORITY
DOCUMENT**

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)



Patent No. 0224228.7
F01/7700 06-0224228.7

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
South Wales
NP10 8QQ

1. Your reference

1/P32658GB

2. Patent application number

(The Patent Office will fill in this part)

0224228.7

3. Full name, address and postcode of the or of each applicant (underline all surnames)

VODAFONE GROUP PLC
THE COURTYARD
2-4 LONDON ROAD, NEWBURY
BERKSHIRE
RG14 1JX

Patents ADP number (if you know it)

If the applicant is a corporate body, give the country/state of its incorporation

U.K.

8154718001

4. Title of the invention

FACILITATING AND AUTHENTICATING TRANSACTIONS

5. Name of your agent (if you have one)

"Address for service" in the United Kingdom to which all correspondence should be sent (including the postcode)

MATHISEN, MACARA & CO.
THE COACH HOUSE
6-8 SWAKELEYS ROAD
ICKENHAM, UXBRIDGE
UB10 8BZ

Patents ADP number (if you know it)

1073001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and (if you know it) the or each application number

Country

Priority application number
(if you know it)

Date of filing
(day / month / year)

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application

Date of filing
(day / month / year)

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? (Answer 'Yes' if:

YES

- a) any applicant named in part 3 is not an inventor, or
 - b) there is an inventor who is not named as an applicant, or
 - c) any named applicant is a corporate body.
- See note (d))

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form

Description	11
Claim(s)	7
Abstract	1
Drawing(s)	2

10. If you are also filing any of the following, state how many against each item.

Priority documents

Translations of priority documents

Statement of inventorship and right to grant of a patent (Patents Form 7/77)

Request for preliminary examination and search (Patents Form 9/77)

1

Request for substantive examination (Patents Form 10/77)

Any other documents (please specify)

11. I/We request the grant of a patent on the basis of this application.

Signature

MATHISEN, MACARA & CO.

Date

17th October 2002

12. Name and daytime telephone number of person to contact in the United Kingdom

MR D.M. FOSTER (01895 678331)

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

- If you need help to fill in this form or you have any questions, please contact the Patent Office on 08459 500505.
- Write your answers in capital letters using black ink or you may type them.
- If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.
- If you have answered 'Yes' Patents Form 7/77 will need to be filed.
- Once you have filled in the form you must remember to sign and date it.
- For details of the fee and ways to pay please contact the Patent Office.

DUPLICATE

FV:P32658GB:021017

UNITED KINGDOM PATENT APPLICATION

APPLICANTS: VODAFONE GROUP PLC

CASE CODE: "SIM Everywhere" (P32658GB)

FORMAL TITLE: FACILITATING AND AUTHENTICATING
TRANSACTIONS.

APPLICATION NO:

FILED:

PRIORITY CLAIMED: NIL

MATHISEN, MACARA & CO.
6 - 8 Swakeleys Road,
Ickenham, Uxbridge,
England, UB10 8BZ

Agents for the Applicants

FACILITATING AND AUTHENTICATING TRANSACTIONS

The invention relates to the facilitation and authentication of transactions. In embodiments of the invention, to be described below in more detail by way of example only, transactions between data processing apparatus (such as a personal computer), or a user thereof, and a (possibly remote) third party are facilitated and authenticated, and such facilitation and authentication may also involve the facilitation and authentication of a payment to be made by or on behalf of the user to the third party.

According to the invention, there is provided a method for authenticating a transaction with data processing apparatus in which the data processing apparatus has operatively associated with it authentication storage means for storing predetermined authentication information, and including the step of carrying out an authentication process via a communications link for authenticating the transaction, the authentication process involving the use of the predetermined authentication information.

According to the invention, there is also provided data processing apparatus in combination with authentication storage means storing predetermined information relating to the authentication of a transaction with the data processing apparatus, the authentication storage means when operatively associated with the data processing apparatus being responsive to an authentication process carried out via a communications link for authenticating the transaction, the authentication process involving the use of the

predetermined information.

According to the invention, there is further provided a data carrier carrying data for use in and by data processing apparatus, the data carrier also incorporating authentication storage means storing predetermined authentication information responsive to an input message for deriving a response dependent on the input message and on the authentication information for use in a remotely operative authentication process for authenticating a transaction involving use of the data carried by the data carrier.

Methods according to the invention of facilitating and authenticating transactions involving data processing apparatus such as a personal computer, data processing apparatus (such as a personal computer) embodying the invention, and data carriers embodying the invention, will now be described, by way of example only, with reference to the accompanying diagrammatic drawings in which:

Figure 1 is a block diagram for explaining the operation of the method in relation to the data processing apparatus; and

Figure 2 is a flow chart for use in the understanding of the block diagram of Figure 1.

There exist many instances when a transaction involving the use of data processing apparatus requires authentication. For example, the data processing apparatus may be

required to carry out a transaction, such as the exchange of information, with a third party, such as a remote third party with which the communication must be made over a telecommunications link (including via the Internet). The third party may require that the data processing apparatus, or the user thereof for the time being, is authenticated to the satisfaction of the third party before the transaction takes place.

As stated, the transaction may merely involve the exchange of information. For example, the user of the data processing apparatus may simply need to be authenticated in order to download information from the third party. Such information may be information kept by the third party on behalf of the user of the data processing apparatus (for example, information relating to the user's bank account). Instead, the information might be information held on other data processing apparatus, such as a data network belonging to an organisation or commercial entity with which the user is connected or by whom the user is employed, thus facilitating access to that network by the user when the user is travelling. Another possible transaction may involve the downloading by the data processing apparatus of software from the remote location.

In addition, the transaction may require a payment to be made by the user in order to enable the transaction to take place, such as a payment to the third party in return for the information provided. Clearly, when such a payment is involved, it is important that the user is authenticated to the satisfaction of the third party and that the payment is made in a safe, simple and secure manner.

Although the foregoing discussion has referred to a "user" of the data processing apparatus, some at least of the transactions described above may not in fact involve any human user: the data processing apparatus may be required to operate automatically (for example, intermittently operating in an information-gathering or monitoring role, and reporting the results to a third party). In such cases, it may also be necessary for the data processing apparatus to authenticate itself to the satisfaction of the third party.

In accordance with a feature of the invention, the data processing apparatus is provided with, or associated with, means (authentication storage means) for storing predetermined authentication information for authenticating that apparatus or a particular user thereof. In one embodiment, the means for storing the predetermined information is removable and can thus be taken by the user and inserted into any data processing apparatus (or computer) which is adapted to receive it, so as to enable that user to be authenticated in respect to a transaction to be carried out by that user with that computer. Advantageously, in such a case the means for storing the predetermined information is in the form of a smart card.

In a more specific example, the smart card is a Subscriber Identity Module or SIM of the type used in and for authenticating the use of handsets in a cellular telecommunications network. Such a network will store details of its users' (subscribers') SIMs. In operation of the network, a user's handset is authenticated (for example, when the user activates the

handset on the network with a view to making or receiving calls) by sending a challenge to the handset incorporating that SIM, in response to which the SIM calculates a reply (dependent on the predetermined information held on the SIM) and transmits it back to the network which checks it against its own information for that user or subscriber in order to complete the authentication process. In the same way, therefore, and in accordance with a feature of the invention, the SIM can be used in or in association with the data processing apparatus or computer so that the same form of authentication process can be carried out. In a case where the SIM is the SIM of a subscriber to a particular cellular telecommunications network, the authentication process can be carried out by that network.

It should be noted that the authentication process being described does not necessarily authenticate the human identity of the user. For example, cellular telecommunication networks have pre-pay subscribers who are issued with SIMs in return for pre-payment enabling them to make calls on the network. However, the identity of such pre-pay subscribers is not known (or not necessarily known) by the networks. Nevertheless, such a user cannot make use of the network until the network has authenticated that user's SIM – that is, has confirmed that that user is a particular user who has a particular pre-paid account with the network. The SIMs of such pre-paid users or subscribers could equally well be used (in the manner described) in or in association with data processing apparatus or computers, for the purposes of authenticating that user.

The SIM need not take the form of a physical (and removable) smart card but instead can be simulated by being embedded in the data processing apparatus or computer in the form of software or represented as a chip for example.

It may be desirable to be able to change the authentication information on the SIM (or simulated SIM) to take account of changed circumstances. For example, the SIM may be a SIM registered with a particular cellular telecommunications network – a network applicable to the country or region where the data processing apparatus or computer is to be used. However, circumstances may arise (for example, the apparatus or the computer is physically moved to a different country or region) in which it is desirable or necessary to re-register the SIM with a different cellular telecommunications network. Ways in which this can be done are disclosed in our co-pending United Kingdom patent applications Nos. 0118406.8, 0122712.3 and 0130790.9 and in our corresponding PCT applications Nos. GB02/003265 and GB02/003260. As described therein in more detail, a SIM (and thus also a simulated SIM) may be initially provided with authentication (and other) information relating to each of a plurality of networks, the information respective to the different networks being selectively activatable.

It is not necessary, however, for the users to be subscribers to a telecommunications method. Instead, they could be subscribers registered with some other centralised system which could then carry out the authentication process in the same way as in a telecommunications network. In such a case, the registration of a SIM (or simulated SIM)

could be transferred from one such centralised system to another in the same manner as described above.

As described above, an aim of the authentication process is to facilitate a transaction between the data processing apparatus or computer and a third party. Where the authentication process is carried out by a telecommunications network, or by some other system, to which the user of the SIM is a subscriber, the satisfactory completion of the authentication process would then be communicated by that network or system to the third party – to enable the transaction to proceed.

For many transactions of the type described, a payment by the user to the third party may be involved. An arrangement as described above, in which the authentication process is carried out by a telecommunications network or other centralised system to which the user is a subscriber advantageously facilitates the making of such payments and is particularly advantageous where (as may often be the case) the payment is for a small amount (for example, payment in return for receipt of information – e.g. weather or traffic information, or for temporary use of specific software); in such a case, the payment can be debited to the account of the subscriber held by the telecommunications network or other centralised system – and then, of course, passed on to the third party, perhaps after deduction of a handling charge.

The block diagram of Figure 1 explains one way of operating the method described

above.

A Windows-based personal computer or PC 10 is shown ('Windows' is a trade mark).. The PC10 is adapted to receive a SIM shown diagrammatically at 12. The SIM may be removably fitted to the PC, for use in identifying a user (that is, the holder of the SIM) or may be fixed within the PC (for identifying the PC itself). The PC 10 incorporates transaction management software 14 which interacts with and controls some of the functions of the SIM.

Also shown in Figure 1 is a cellular telephone network 16, such as the Vodafone (trade mark) network, and it is assumed that the SIM 12 is registered with the network 16.

The operation of the system shown in Figure 1 will be explained in relation to the flow chart of Figure 2.

At step A, the user of the PC 10 requests use of a particular application 17 on the PC. For example, the user might wish to view web pages containing specialised information which are encrypted and thus not generally available. In order to do this, the user requests a "session key" – that is, permission to carry out a transaction involving time-limited use of the particular application. The request for the session key is addressed to the transaction manager 14. The transaction manager 14 then, transmits identification information derived from the SIM 12 (an "I am here" message) to the security services

part 18 of the network 16 (step B). In response to the "I am here" message, the network transmits a random challenge (step C) to the transaction manager 14, this challenge being based on information known to the network about the SIM 12.

At step D, the transaction manager 14 responds to the challenge by providing an answer derived from the challenge and the key held on the SIM. The reply is checked by the security services part 18 of the network 16. Assuming that the response is satisfactory, the security services part 18 authenticates the user and confirms this to the transaction manager 14 (step E). At the same time, the security services part 18 in the network transmits the session key (step F) to the application services part 22 of the network 16.

The transaction manager 14 also transmits the session key to the application 17 (step G).

The user can now make the request for the particular application (step H), accompanying this application request with the session key received at step G. The application request of step H is transmitted to an application services part 22 which may be part of the network 16 (as shown) or may be separate and controlled by a third party. At step I the application services part compares the session key received with the application request (step H) with the session key received at step F. Assuming that the result of this check is satisfactory, the application services part 22 now transmits acceptance of the application request (step J) to the PC 10, and the application now proceeds (time limited).

The network can now debit the user's account with a charge for the session.

The foregoing is of course merely one example of an implementation of what has been described.

According to another aspect of the invention, a data carrier may be provided with means for storing predetermined information such as in one of the forms described above – that is, a SIM or (more probably) software simulating a SIM. The simulated SIM is associated with data stored on the data carrier. The data carrier may, for example, be a DVD or CD ROM or some other similar data carrier, and the data thereon may be software or a suite of software.

According to a feature, the simulated SIM may be used to identify and authenticate the data (such as the software) on the data carrier. The simulated SIM will be registered with a telecommunications network or some other centralised system, in the same manner as described above. When the data carrier is placed in data processing apparatus such as a computer, for use therein, the SIM would be used to identify and authenticate the data carrier and the data stored thereon and (for example) could then permit the software to be downloaded for use in the computer. In this way, the SIM could be used subsequently to block further use of the software (for example, in another computer), or to allow the data to be used for only a predetermined number of times (whether in the same or in a different computer). If, for example, the data carrier (with its SIM) is placed in a computer which has also received a particular user's SIM then (a) the SIM on the data carrier can be used

to identify and authenticate the software and (b) the SIM in or associated with the computer can be used to authenticate the user and could subsequently be used to enable a charge to be debited to that user as payment for use of the software.

CLAIMS

1. A method for authenticating a transaction with data processing apparatus in which the data processing apparatus has operatively associated with it authentication storage means for storing predetermined authentication information, and including the step of carrying out an authentication process via a communications link for authenticating the transaction, the authentication process involving the use of the predetermined authentication information.
2. A method according to claim 1, in which the transaction is a transaction involving use of the data processing functions of the data processing apparatus.
3. A method according to claim 1 or 2, in which there is a plurality of the authentication storage means.
4. A method according to claim 3, in which the step of carrying out the authentication process is at least partly carried out by authentication means which is common to all the authentication storage means of the said plurality thereof.
5. A method according to claim 3 or 4, in which each authentication storage means is associated with a specific data processing apparatus.

6 A method according to claim 1 or 2, in which there is a plurality of the authentication storage means each respective to a particular one of a plurality of specified users of the data processing apparatus, and in which the authentication process involving the use of the predetermined information from a particular one of the authentication storage means authenticates a transaction by the one of the specified users which is respective to that authentication storage means.

7. A method according to claim 6, in which the step of carrying out the authentication process is at least partly carried out by authentication means which is common to all the users.

8. A method according to claim 7, in which the authentication means which is common to all the users is authentication means which is part of a system with which all the authentication storage means are registered.

9. A method according to claim 8, in which the system is a telecommunications network and in which the predetermined information stored by the authentication storage means for each user corresponds to information used to authenticate that user in relation to the telecommunications network.

10. A method according to claim 8 or 9, in which each user is authenticated in the system by means of the use of a smart card or subscriber identity module (e.g. SIM), and

in which the authentication storage means respective to that user corresponds to or simulates the smart card for that user.

11. A method according to any one of claims 8 to 10, including the step of registering one or more of the authentication storage means with a different system.

12. A method according to any preceding claim, in which the authentication storage means is associated with the data processing apparatus by being associated with data or software for use by that data processing apparatus.

13. A method according to claim 12, in which the authentication storage means is incorporated on a data carrier for the data or software.

14. A method according to any preceding claim, in which the authentication process involves the sending of a message and the generation of a response dependent on the message and the predetermined information.,

15. A method according to any preceding claim, including the step of levying a charge for the transaction when authenticated.

16. A method according to any one of claims 8 to 11, including the step of levying a charge for the transaction when authenticated, the step of levying the charge being carried

out by the said system.

17. A method according to any preceding claim, in which the data processing apparatus is a personal computer.

18. Data processing apparatus in combination with authentication storage means storing predetermined information relating to the authentication of a transaction with the data processing apparatus, the authentication storage means when operatively associated with the data processing apparatus being responsive to an authentication process carried out via a communications link for authenticating the transaction, the authentication process involving the use of the predetermined information.

19. Apparatus according to claim 18, in which the transaction is a transaction involving use of the data processing functions of the data processing apparatus.

20. Apparatus according to claim 18 or 19, in which the authentication storage means is specific to the data processing apparatus.

21. Apparatus according to claim 18 or 19, in which there is a plurality of the authentication storage means each for storing predetermined authentication information respective to any one of a plurality of specified users and each relating to the authentication of a transaction with the data processing apparatus by the respective one of

the specified users.

22. Apparatus according to claim 21, including remote authentication means for at least partly carrying out the authentication process and which is part of a system with which all the users are registered.

23. Apparatus according to claim 22, in which the system is a telecommunications network and in which the predetermined authentication information respective to each user corresponds to information used to authenticate that user within the telecommunications network.

24. Apparatus according to claim 22, in which each user is authenticated in the system by means of the use of a subscriber identity module (SIM) in the form of a smart card, and in which the authentication storage means respective to that user corresponds to or simulates the subscriber identity module for that user.

25. Apparatus according to any one of claims 18 to 24, in which the authentication process involves the sending of a message and the generation of a response dependent on the message and the predetermined information.

26. A data carrier carrying data for use in and by data processing apparatus, the data carrier also incorporating authentication storage means storing predetermined

authentication information responsive to an input message for deriving a response dependent on the input message and on the authentication information for use in a remotely operative authentication process for authenticating a transaction involving use of the data carried by the data carrier.

27. A data carrier according to claim 26, in which the data carried by the data carrier includes software.

28. A data carrier according to claim 26 or 27, in which the authentication storage means is one of a plurality of such authentication storage means which are registered with a common system, including authentication means for carrying out the authentication process.

29. A data carrier according to claim 28, in which the common system is a telecommunications network.

30. A data carrier according to claim 29, in which the telecommunications network has a plurality of users registered therewith which are authenticated therein by means of the use of respective subscriber identity modules (SIMs) in the form of smart cards, and in which the authentication storage means corresponds to or simulates such a subscriber identity module.

31. A method for authenticating a transaction with data processing apparatus, substantially as described with reference to the accompanying drawings.

32. Data processing apparatus, substantially as described with reference to the accompanying diagrammatic drawing.

33. A data carrier, substantially as described with reference to the accompanying drawings.

ABSTRACT (Figure 1)

A computer, such as a Windows-based PC (10), has associated with it a Subscriber Identity Module (or SIM) (12), such as of the type used in a GSM cellular telephone system. The SIM (12) can be authenticated by the telephone network, in the same way as for authenticating SIMs of telephone handset users in the network, and can in this way authenticate the user of the PC (10) or the PC (10) itself. Such authentication can, for example, permit use of the PC (10) for a time-limited session in relation to a particular application which is released to the PC (10) after the authentication is satisfactorily completed. The application may be released to the PC (10) by a third party after and in response to the satisfactory completion of the authentication process. A charge for the session can be debited to the user by the telecommunications network and then passed on to the third party.

1/2

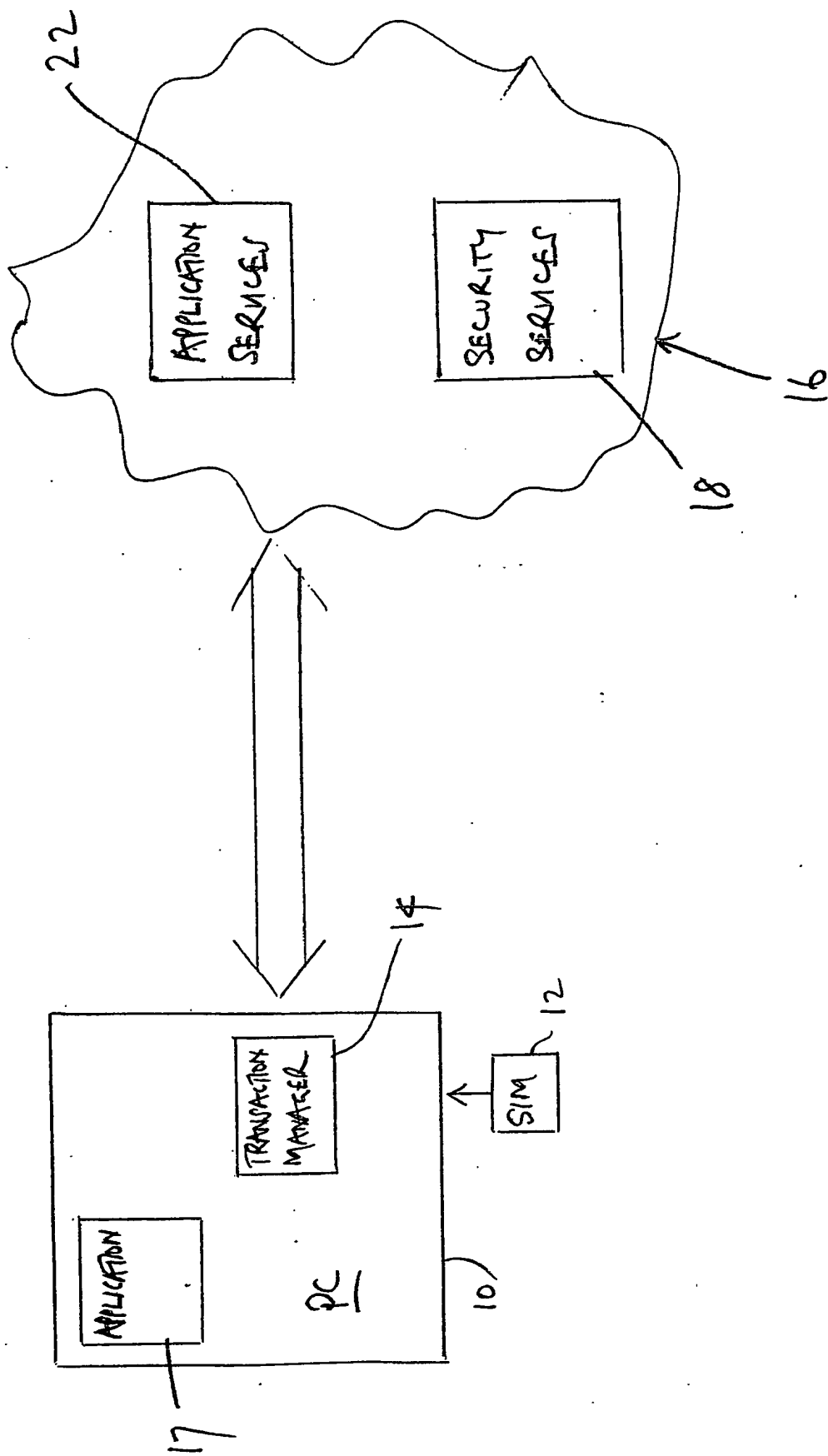


Fig. 1

2/2

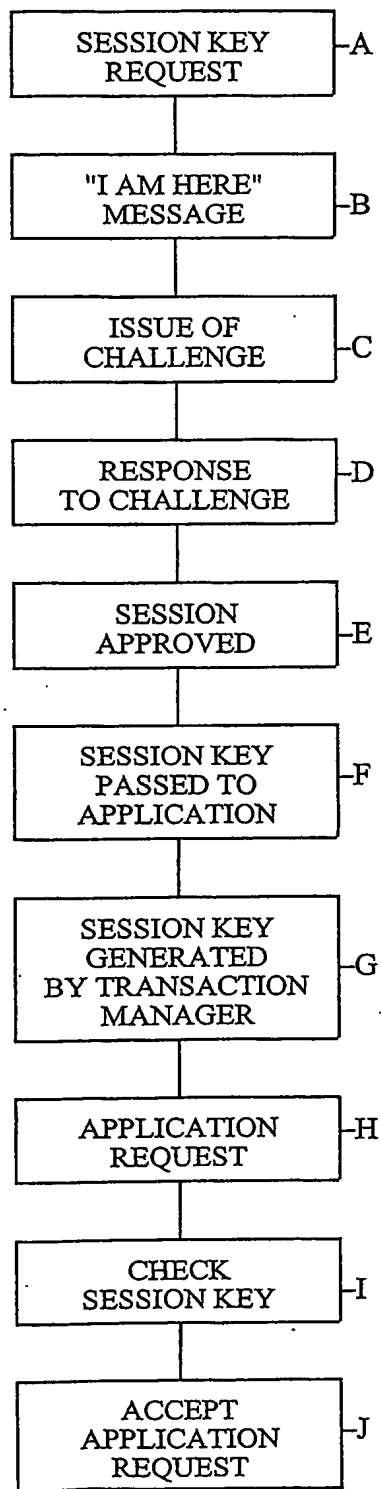


Fig. 2